03500.017468. PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	:	Examiner: Not Yet Assigned
HIROHIDE TACHIKAWA	)	
	:	Group Art Unit: 2131
Application No.: 10/616,941	)	
	:	
Filed: July 11, 2003	)	
	:	
For: NETWORK CONFIGURATION METHOD AND COMMUNICATION SYSTEM AND APPARATUS	)	January 26, 2004

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

SUBMISSION OF PRIORITY DOCUMENT

Sir:

In support of Applicant's claim for priority under 35 U.S.C. § 119, enclosed is a certified copy of the following foreign application:

2002-233119 filed August 9, 2002.

Applicant's undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our address given below.

Respectfully submitted,

Attorney for Applicant

Registration No. 42476

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200
40249v1

2-6

CFO 17468 US/kh
10/616,941

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００２年 ８月 ９日

出 願 番 号
Application Number: 特願２００２－２３３１１９

[ST. 10/C]: [ＪＰ２００２－２３３１１９]

出 願 人
Applicant(s): キヤノン株式会社

２００３年 ８月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０６７１４０

【書類名】　特許願
【整理番号】　4771006
【提出日】　平成14年 8月 9日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/00
【発明の名称】　無線接続方法、無線接続システムおよびアクセスポイント装置
【請求項の数】　27
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
【氏名】　立川　博英
【特許出願人】
【識別番号】　000001007
【氏名又は名称】　キヤノン株式会社
【代表者】　御手洗　冨士夫
【代理人】
【識別番号】　100081880
【弁理士】
【氏名又は名称】　渡部　敏彦
【電話番号】　03(3580)8464
【手数料の表示】
【予納台帳番号】　007065
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9703713

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　無線接続方法、無線接続システムおよびアクセスポイント装置

【特許請求の範囲】

【請求項１】　認証サーバ機能および認証用データの生成機能を有するアクセスポイント装置の無線接続方法において、

前記アクセスポイント装置とクライアント端末との間で、認証プロセスを必要としない第１の暗号化手段による無線通信のリンクを確立するステップと、

前記第１の暗号化手段による無線通信のリンクが確立した状態で、前記認証用データを前記クライアント端末に送付するステップと、

該認証用データを送付した後、前記第１の暗号化手段による無線通信のリンクを一旦破棄するステップと、

前記クライアント端末に送付された認証用データを用い、認証プロセスを必要とする第２の暗号化手段による無線通信に移行するステップとを有することを特徴とする無線接続方法。

【請求項２】　前記第１の暗号化手段による無線通信のリンクを確立するために、前記クライアント端末から所定の入力操作を受け付けるステップを有することを特徴とする請求項１記載の無線接続方法。

【請求項３】　前記所定の入力操作を、前記アクセスポイント装置に付属する表示手段、あるいは該アクセスポイント装置とネットワーク接続されたクライアント端末上で動作するブラウザに表示するステップを有することを特徴とする請求項１記載の無線接続方法。

【請求項４】　前記第１の暗号化手段による無線通信のリンクを確立した際、前記クライアント端末の識別データを前記アクセスポイント装置に送信するステップを有することを特徴とする請求項１記載の無線接続方法。

【請求項５】　前記送信された識別データを、前記アクセスポイント装置に付属する表示手段、あるいは該アクセスポイント装置とネットワーク接続されたクライアント端末上で動作するブラウザに一覧表示するステップと、

前記一覧表示された識別データに対応するクライアント端末の編集・確認を促すステップとを有し、

前記送付するステップでは、確認されたクライアント端末に対し、前記認証用データを送付することを特徴とする請求項４記載の無線接続方法。

【請求項６】　前記一覧表示されたクライアント端末の確認が終了した場合、該確認されたクライアント端末固有の識別情報を、前記アクセスポイント装置内のアドレスフィルタに自動設定するステップを有し、

前記アドレスフィルタへの自動設定により、前記確認されたクライアント端末以外のアクセスポイント装置への接続を禁止し、所定の復帰手順がとられない限り、前記接続の禁止状態を維持することを特徴とする請求項５記載の無線接続方法。

【請求項７】　前記所定の入力操作はアクセスポイント識別情報の入力であり、該アクセスポイント識別情報は前記第２の暗号化手段による無線通信に移行する際にも使用されることを特徴とする請求項２記載の無線接続方法。

【請求項８】　前記認証用データは認証サーバ用証明書データであることを特徴とする請求項１、２、５または７記載の無線接続方法。

【請求項９】　認証サーバ機能および認証用データの生成機能を有するアクセスポイント装置とクライアント端末との間で無線通信を行う無線接続システムにおいて、

前記アクセスポイント装置と前記クライアント端末との間で、認証プロセスを必要としない第１の暗号化手段による無線通信のリンクを確立する確立手段と、

前記第１の暗号化手段による無線通信のリンクが確立した状態で、前記認証用データを前記クライアント端末に送付する送付手段と、

該認証用データを送付した後、前記第１の暗号化手段による無線通信のリンクを一旦破棄する破棄手段と、

前記クライアント端末に送付された認証用データを用い、認証プロセスを必要とする第２の暗号化手段による無線通信に移行する移行手段とを備えたことを特徴とする無線接続システム。

【請求項１０】　前記第１の暗号化手段による無線通信のリンクを確立するために、前記クライアント端末から所定の入力操作を受け付ける受付手段を備えたことを特徴とする請求項９記載の無線接続システム。

【請求項１１】　前記所定の入力操作を、前記アクセスポイント装置に付属する表示手段、あるいは該アクセスポイント装置とネットワーク接続されたクライアント端末上で動作するブラウザに表示する表示制御手段を備えたことを特徴とする請求項９記載の無線接続システム。

【請求項１２】　前記第１の暗号化手段による無線通信のリンクを確立した際、前記クライアント端末の識別データを前記アクセスポイント装置に送信する送信手段を備えたことを特徴とする請求項９記載の無線接続システム。

【請求項１３】　前記送信された識別データを、前記アクセスポイント装置に付属する表示手段、あるいは該アクセスポイント装置とネットワーク接続されたクライアント端末上で動作するブラウザに一覧表示する第２の表示制御手段と、

前記一覧表示された識別データに対応するクライアント端末の編集・確認を促す督促手段とを備え、

前記送付手段は、確認されたクライアント端末に対し、前記認証用データを送付することを特徴とする請求項１２記載の無線接続システム。

【請求項１４】　前記一覧表示されたクライアント端末の確認が終了した場合、該確認されたクライアント端末固有の識別情報を、前記アクセスポイント装置内のアドレスフィルタに自動設定する自動設定手段を備え、

前記アドレスフィルタへの自動設定により、前記確認されたクライアント端末以外のアクセスポイント装置への接続を禁止し、所定の復帰手順がとられない限り、前記接続の禁止状態を維持することを特徴とする請求項１３記載の無線接続システム。

【請求項１５】　前記所定の入力操作はアクセスポイント識別情報の入力であり、該アクセスポイント識別情報は前記第２の暗号化手段による無線通信に移行する際にも使用されることを特徴とする請求項１０記載の無線接続システム。

【請求項１６】　前記認証用データは認証サーバ用証明書データであることを特徴とする請求項９、１０、１３または１５記載の無線接続システム。

【請求項１７】　認証サーバ機能および認証用データの生成機能を有し、クライアント端末との間で無線通信を行うアクセスポイント装置において、

前記クライアント端末との間で、認証プロセスを必要としない第１の暗号化手段による無線通信のリンクを確立する確立手段と、

前記第１の暗号化手段による無線通信のリンクが確立した状態で、前記認証用データを前記クライアント端末に送付する送付手段と、

該認証用データを送付した後、前記第１の暗号化手段による無線通信のリンクを一旦破棄する破棄手段と、

前記クライアント端末に送付された認証用データを用い、認証プロセスを必要とする第２の暗号化手段による無線通信に移行する移行手段とを備えたことを特徴とするアクセスポイント装置。

【請求項１８】　前記第１の暗号化手段による無線通信のリンクを確立するために、前記クライアント端末から所定の入力操作を受け付ける受付手段を備えたことを特徴とする請求項１７記載のアクセスポイント装置。

【請求項１９】　前記所定の入力操作を、付属の表示手段、あるいはネットワーク接続されたクライアント端末上で動作するブラウザに表示する表示制御手段を備えたことを特徴とする請求項１７記載のアクセスポイント装置。

【請求項２０】　前記第１の暗号化手段による無線通信のリンクを確立した際、前記クライアント端末から送信された該クライアント端末の識別データを受信する受信手段を備えたことを特徴とする請求項１７記載のアクセスポイント装置。

【請求項２１】　前記受信した識別データを、付属の表示手段、あるいはネットワーク接続されたクライアント端末上で動作するブラウザに一覧表示する第２の表示制御手段と、

前記一覧表示された識別データに対応するクライアント端末の編集・確認を促す督促手段とを備え、

前記送付手段は、確認されたクライアント端末に対し、前記認証用データを送付することを特徴とする請求項２０記載のアクセスポイント装置。

【請求項２２】　前記一覧表示されたクライアント端末の確認が終了した場合、該確認されたクライアント端末固有の識別情報を、前記アクセスポイント装置内のアドレスフィルタに自動設定する自動設定手段を備え、

前記アドレスフィルタへの自動設定により、前記確認されたクライアント端末以外のアクセスポイント装置への接続を禁止し、所定の復帰手順がとられない限り、前記接続の禁止状態を維持することを特徴とする請求項２１記載のアクセスポイント装置。

【請求項２３】　前記所定の入力操作はアクセスポイント識別情報の入力であり、該アクセスポイント識別情報は前記第２の暗号化手段による無線通信に移行する際にも使用されることを特徴とする請求項１８記載のアクセスポイント装置。

【請求項２４】　前記認証用データは認証サーバ用証明書データであることを特徴とする請求項１７、１８、２１または２３記載のアクセスポイント装置。

【請求項２５】　複数の無線通信方式に対応するため、無線通信拡張インターフェースを少なくとも１つ備え、該無線通信拡張インターフェースに、所望の無線通信方式に対応した無線通信拡張カードを装着することによって、前記所望の無線通信方式で前記クライアント端末との無線通信を実現することを特徴とする請求項１７記載のアクセスポイント装置。

【請求項２６】　前記無線通信拡張インターフェースと、基幹ネットワークに接続するためのインターフェースとを別々に備え、前記無線通信拡張インターフェースに接続されたクライアント端末と前記基幹ネットワークとのルーティング処理を行うことを特徴とする請求項２５記載のアクセスポイント装置。

【請求項２７】　ルーティング処理を行うＣＰＵと同一のＣＰＵで、前記認証サーバ機能および前記認証用データの生成機能を実現することを特徴とする請求項２６記載のアクセスポイント装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、無線ＬＡＮ（ＩＥＥＥ８０２．１１）やＢｌｕｅｔｏｏｔｈ等の無線通信機能を有する端末を用いて、安全なＰｅｒｓｏｎａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ（ＰＡＮ）を構築する場合などに用いられる無線接続方法、無線接続システムおよびアクセスポイント装置に関する。

【０００２】

【従来の技術】

従来、無線ＬＡＮやＢｌｕｅｔｏｏｔｈでは、その通信媒体として電波を用いるので、通信先の制限が難しかった。このため、これらの規格では、通信先毎に暗号鍵を変更することで、たとえパケットをのぞき見られても、それを解読できないようにするといった防御手段がとられてきた。現在、最も一般的な無線通信暗号化手段は、ＩＥＥＥ８０２．１１方式の場合、ＷＥＰキー（４０ｂｉｔ，１２８ｂｉｔ）による暗号化であり、Ｂｌｕｅｔｏｏｔｈ方式の場合、Ｐｉｎコードから自動生成される１２８ｂｉｔの暗号鍵（１２８ｂｉｔ）による暗号化である。

【０００３】

しかし、これらの暗号化方式は脆弱性を有することが指摘されており、無線通信の安全性を更に高めるための暗号化方式として、８０２．１１方式では、８０２．１ｘベースの認証を実施した上での動的ＷＥＰキー変換（ＥＡＰ）や、ＴＫＩＰ，ＡＥＳといった更に高度な暗号化方式、Ｂｌｕｅｔｏｏｔｈ方式では、８０２．１ｘベースの上位アプリケーション層での認証・暗号化方式などが検討され、一部実施されている。

【０００４】

この中でも８０２．１ｘをベースとしたＥＡＰ（Ｅｘｔｅｎｓｉｂｌｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ、拡張可能認証プロトコル）方式と呼ばれる認証・暗号化手段は、一部のＯＳ環境において、８０２．１１方式向けの認証・暗号化手段として標準で実装されている。

【０００５】

無線ＬＡＮ（８０２．１１）におけるＥＡＰ方式では、クライアントの端末がネットワーク接続要求を行う際、ＴＣＰ／ＩＰを利用してイントラネット内に設けられた認証サーバ（ＲＡＤＩＵＳサーバ等）とデータ通信を行い、認証サーバからクライアントへの証明書の要求またはチャレンジを実施する。

【０００６】

クライアントは、証明書所有の証明を行うか、チャレンジに対してアカウント

名とパスワードを返し、それらが認証サーバ内のデータと一致した場合、認証サーバは、無線通信を暗号化するための１２８ｂｉｔの暗号鍵または暗号鍵生成手段を、アクセスポイントおよびクライアントに返す。このようなプロセスを経て、クライアントが認証をパスすると、それ以降の無線通信は、クライアントとアクセスポイントとの両者間で、１２８ｂｉｔの暗号鍵をＷＥＰキーとして利用することで、暗号化される。さらに、上記プロセスは一定時間毎に定期的に実施され、暗号鍵の更新が行われる。

【０００７】

また、Ｂｌｕｅｔｏｏｔｈ方式では、ＰＡＮプロファイルにおいて、セキュリティ向上のために、８０２．１ｘ認証・暗号化手段を用いることが推奨されている。Ｂｌｕｅｔｏｏｔｈの場合、無線媒体である電波を暗号化するための鍵の生成は、Ｂｌｕｅｔｏｏｔｈ方式で通信を行うデバイス間のＰｉｎコードによる相互認証によって自動的に行われるので、認証サーバから受け取った暗号鍵情報を、無線ＬＡＮにおけるＷＥＰキーのように、電波そのものの暗号化鍵として利用できないが、無線媒体としての電波を生成する前段階で、パケットを暗号化する際の鍵として利用できる。これにより、二重に暗号化して通信のセキュリティを向上させることができる。

【０００８】

このように、８０２．１ｘ方式の認証・暗号化プロセスでは、認証を実施するための認証サーバがネットワーク内に存在し、同サーバでクライアントのアカウントを集中管理する。このため、８０２．１ｘ方式を用いることで、クライアントがどこにいても、認証サーバとのＴＣＰ／ＩＰによる通信が実施可能である限り、同一のアカウント・パスワードを用いてイントラネット等のネットワークに接続することができる。

【０００９】

【発明が解決しようとする課題】

しかしながら、上記従来の無線接続システムでは、上記８０２．１ｘ方式による認証・暗号化プロセスを用いることで、クライアントは無線通信による安全なネットワーク接続を実現できるが、このために、ネットワーク内に認証サーバを

設置し、かつこの認証サーバに予めクライアントのアカウントを登録しておく必要がある。

【００１０】

すなわち、８０２．１ｘ方式は、比較的規模の大きなイントラネット等における運用を想定した方式であり、無線によるネットワーク接続を行うクライアントも、認証サーバ上にアカウントを持ったメンバに限定されるという制限があった。

【００１１】

このため、認証サーバにアカウントの無い外来者が参加するミーティングを行う場合、あるいはイントラネットへの接続手段がない社外の会議室等でのミーティングを行う場合、８０２．１ｘ方式による認証・暗号化プロセスを利用した無線通信による安全なネットワーク構築ができないという不具合があった。

【００１２】

尚、このような場合、認証・暗号化を無くした無線通信を行うことは実現可能であるが、セキュリティの面から大きな問題があることは勿論である。また、手作業による無線通信用パラメータの設定を実施するようにした場合、無線通信の暗号化は可能であるが、クライアントはイントラネット内で通常利用する８０２．１ｘ方式のアカウント・パスワードの入力による自動接続とは、全く異なる接続手段を手動で行わなければならず、操作方法に統一性が無く、煩雑であり、利便性が損なわれる。

【００１３】

そこで、本発明は、８０２．１ｘ認証・暗号化方式などの認証プロセスを要する、比較的安全性の高い暗号化方式による無線通信を用いたＰＡＮ構築を、認証プロセスに対応したアカウントや証明書を事前に所有していないクライアント端末においても実現可能である無線接続方法、無線接続システムおよびアクセスポイント装置を提供することを目的とする。

【００１４】

【課題を解決するための手段】

上記目的を達成するために、本発明の無線接続方法は、認証サーバ機能および

認証用データの生成機能を有するアクセスポイント装置の無線接続方法において、前記アクセスポイント装置とクライアント端末との間で、認証プロセスを必要としない第１の暗号化手段による無線通信のリンクを確立するステップと、前記第１の暗号化手段による無線通信のリンクが確立した状態で、前記認証用データを前記クライアント端末に送付するステップと、該認証用データを送付した後、前記第１の暗号化手段による無線通信のリンクを一旦破棄するステップと、前記クライアント端末に送付された認証用データを用い、認証プロセスを必要とする第２の暗号化手段による無線通信に移行するステップとを有することを特徴とする。

【００１５】

本発明の無線接続システムは、認証サーバ機能および認証用データの生成機能を有するアクセスポイント装置とクライアント端末との間で無線通信を行う無線接続システムにおいて、前記アクセスポイント装置と前記クライアント端末との間で、認証プロセスを必要としない第１の暗号化手段による無線通信のリンクを確立する確立手段と、前記第１の暗号化手段による無線通信のリンクが確立した状態で、前記認証用データを前記クライアント端末に送付する送付手段と、該認証用データを送付した後、前記第１の暗号化手段による無線通信のリンクを一旦破棄する破棄手段と、前記クライアント端末に送付された認証用データを用い、認証プロセスを必要とする第２の暗号化手段による無線通信に移行する移行手段とを備えたことを特徴とする。

【００１６】

本発明のアクセスポイント装置は、認証サーバ機能および認証用データの生成機能を有し、クライアント端末との間で無線通信を行うアクセスポイント装置において、前記クライアント端末との間で、認証プロセスを必要としない第１の暗号化手段による無線通信のリンクを確立する確立手段と、前記第１の暗号化手段による無線通信のリンクが確立した状態で、前記認証用データを前記クライアント端末に送付する送付手段と、該認証用データを送付した後、前記第１の暗号化手段による無線通信のリンクを一旦破棄する破棄手段と、前記クライアント端末に送付された認証用データを用い、認証プロセスを必要とする第２の暗号化手段

による無線通信に移行する移行手段とを備えたことを特徴とする。

【００１７】

【発明の実施の形態】

本発明の無線接続方法、無線接続システムおよびアクセスポイント装置の実施の形態について図面を参照しながら説明する。

【００１８】

［第１の実施形態］

図１は第１の実施形態におけるアクセスポイント装置およびクライアント端末によって構築されるネットワークシステムを示す図である。図において、１はＩＥＥＥ８０２．１１やＢｌｕｅｔｏｏｔｈ等の規格を用いた無線通信手段により、安全なネットワークを構築するアクセスポイントである。２はアクセスポイント１に内蔵された無線通信部である。３はアクセスポイント１に内蔵された認証サーバである。４はアクセスポイント１に内蔵された証明書サーバである。５はアクセスポイント１からクライアント端末へのメッセージを表示する表示部である。

【００１９】

６はＩＥＥＥ８０２．１１やＢｌｕｅｔｏｏｔｈ等の無線通信手段である。７、８はアクセスポイント１と無線接続されるＰＤＡである。９、１０はアクセスポイント１と無線接続されるノートＰＣである。

【００２０】

図２はアクセスポイント１の構成を示すブロック図である。図において、１０１はＣＰＵである。１０２はメモリコントローラやバス変換機能を有するノースブリッジチップである。１０３はノースブリッジチップ１０２から出力される高速バスを更に低速の汎用バスに変換するサウスブリッジである。

【００２１】

１０４はＲＡＭである。１０５は表示用グラフィックチップである。１０６は表示装置である。表示用グラフィックチップ１０５および表示装置１０６は図１の表示部５を構成する。１０７はプログラムや様々な設定情報を記憶するＲＯＭである。１０８、１０９はＰＣＩバスからＣａｒｄｂｕｓ等の標準拡張バスへの

変換を行うブリッジチップである。１１０、１１１、１１２、１１３は無線通信拡張カードを挿入することによって様々な無線通信方式に対応する拡張バスインターフェースである。

【００２２】

１１４はカスケード接続用ＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）である。１１５はカスケード接続用ＰＨＹ（Ｐｈｙｓｉｃａｌ　ｌａｙｅｒ）である。１１６はカスケード接続用８０２．３ｕインターフェースである。１１７は有線ネットワークによるＰＡＮ構築用ＭＡＣである。１１８は有線ネットワークによるＰＡＮ構築用スイッチングコントローラである。１１９、１２０、１２１、１２２は有線ネットワークによるＰＡＮ構築用インターフェースである。１２３は上記回路に電源を供給する電源装置である。

【００２３】

拡張バスインターフェース１１０、１１１、１１２、１１３は全て同等の機能を有しており、このインターフェースに無線通信機能を有する拡張カードを挿入することによって、拡張カードはアクセスポイントとして機能する。また、複数の拡張バスインターフェースを装備し、Ｂｌｕｅｔｏｏｔｈ、８０２．１１ｂ、８０２．１１ａ等それぞれに異なる無線通信手段に対応した無線通信拡張カードを挿入することで、１台で複数の無線通信手段に同時に対応可能なアクセスポイントを構築することができる。さらに、同一の通信手段に対応した無線通信拡張カードを複数挿入すると、１枚の無線通信拡張カードで対応可能なユーザ数を越えた数のユーザに、１台のアクセスポイント装置で対応することができる。また、アクセスポイントを経由して基幹ネットワークに接続する無線通信のクライアント端末に対し、ユーザ毎のルーティングやフィルタリングを行うことで、不正なアクセスを相互に禁止できる。さらに、単一のＣＰＵ１０１およびその周辺回路で、アクセスポイントのルーティング機能、認証サーバ機能、および認証サーバ用アカウントあるいは証明書生成機能（証明書サーバ機能）を実現することで、製品化する場合のコストを低減できる。

【００２４】

図３はアクセスポイント装置のソフトウェアの構成を示す図である。認証サー

バ（ＲＡＤＩＵＳサーバ等）のエミュレーション機能やアクセスポイントを実現するためのＴＣＰ／ＩＰスタック等を、図２の本体側ブロック（Ｍａｉｎ　Ｂｏａｒｄ）に設けることによって、種類の異なる無線通信手段への対応を柔軟に行い、かつシステムの総コストを抑えることができる。

【００２５】

つぎに、上記構成を有するアクセスポイント１を利用し、無線通信によるＰＡＮを構築する動作を示す。無線通信によるＰＡＮを構築する際、アクセスポイント１に対する起動操作か、あるいは何らかのスイッチ入力を行うと、アクセスポイント１は、低レベルな暗号化を施した無線接続を確立するために必要な情報を、表示部５に表示する。このときの表示は、ＥＳＳ　ＩＤ、ＷＥＰキー、あるいはＰｉｎコード等の８０２．１１やＢｌｕｅｔｏｏｔｈによる無線通信を暗号化するためのパラメータそのものでもよい。また、ユーザが所有するクライアント端末７、８、９、１０に、予めインストールされたプログラムによって、上記無線通信を暗号化するためのパラメータに自動変換を行うためのキーワードであってもよい。

【００２６】

図４は８０２．１１方式による無線接続を確立する処理手順を示すフローチャートである。まず、前述したように、新しいＰＡＮの構築要求が、アクセスポイント１の起動やスイッチ入力によって行われるまで待機し（ステップＳ１）、ＰＡＮの構築要求が行われた場合、アクセスポイント１は、８０２．１１方式による低レベルの暗号化を施した無線通信に必要なパラメータであるＥＳＳ　ＩＤとＷＥＰキーを表示する（ステップＳ２）。

【００２７】

ここで、ＰＡＮに接続しようとするユーザは、これらの表示されたパラメータを、各自が所有するクライアント端末７、８、９、１０に手入力する。この操作によって、低レベルな暗号化を施した無線通信が、アクセスポイント１とクライアント端末７、８、９、１０との間に確立される。

【００２８】

尚、このとき、ＴＣＰ／ＩＰベースの接続を確立する必要があるので、低レベ

ルの暗号化を施した無線レベルでのリンクが確立した後、アクセスポイント１に内蔵されたＤＨＣＰ機能等を用い、各クライアント端末７、８、９、１０は、ＩＰアドレスの自動発行等の処理を行い、ＴＣＰ／ＩＰによるネットワーク接続を確立する。

【００２９】

その後、アクセスポイント１は、自身に無線接続されているクライアント端末７、８、９、１０の情報を、アクセスポイント１の表示部５に一覧表示する（ステップＳ３）。このとき表示されるクライアント端末の情報は、接続されている無線端末のハードウェア識別コードでもよいが、その場合、ＰＡＮの管理責任者は、不正アクセス者の特定等のために、各クライアント端末の持つハードウェア識別コードを事前に把握しておく必要がある。

【００３０】

しかし、ハードウェア識別コードの管理は、ユーザにとって非常に煩雑である。そこで、ＰＡＮを構築しようとするユーザは、事前に自身が所有するクライアント端末７、８、９、１０に、ＰＡＮ構築を支援するためのソフトウェアをインストールしておき、このとき、クライアント端末利用者の氏名や所属などの個人識別情報を入力しておくものとする。このような処理を施しておき、低レベルの暗号化を施した無線接続を確立した際、各クライアント端末７、８、９、１０からアクセスポイント１に個人識別情報を送信することによって、アクセスポイント１は、自身に無線接続されているクライアント端末７、８、９、１０の個人識別情報を一覧表示することができる。

【００３１】

図５は個人識別情報の一覧表示を示す図である。ＰＡＮの管理責任者は、無線通信によって接続されているユーザの一覧表示を見ながら、任意に編集し、不正なＰＡＮ参加者がいないことを目視で確認すると、アクセスポイント１に対し、ＰＡＮ参加者の確認作業が完了したことを示すためのスイッチ入力等を行う。すなわち、ステップＳ３で無線接続されているクライアント端末７、８、９、１０の個人識別情報を一覧表示した後、修正要求があるか否かを判別し（ステップＳ４）、修正要求がある場合、修正作業を行って（ステップＳ５）、ステップＳ３

の処理に戻る。一方、修正要求がないとして、確認作業完了が入力された場合、そのままステップＳ６の処理に移行する。

【００３２】

アクセスポイント１は、確認作業完了が入力された場合、確認されたユーザ以外のＰＡＮ参加を拒絶するため、確認されたユーザのＭＡＣアドレス等を用いたハードウェア識別コードによるフィルタリング設定を行う（ステップＳ６）。尚、このフィルタリング設定は、一般的な無線ＬＡＮアクセスポイントが有するＭＡＣアドレスによるユーザ制限機能を用いることにより、確認されたユーザ名のＭＡＣアドレスを自動設定する等の処理で実現できる。

【００３３】

また、アクセスポイント１は、同時に確認済みの全てのクライアント端末に対する認証用アカウントまたは証明書の発行作業を行う（ステップＳ７）。全てのクライアント端末に認証用アカウントまたは証明書を送信し（ステップＳ８）、送信が完了したか否かを判別する（ステップＳ９）。送信が完了すると、アクセスポイント１は、一旦、現状の低レベルな暗号化を施した無線通信によるリンクを破棄し（ステップＳ１０）、認証処理を要する高レベルな暗号化を施した無線通信の開始に備え、本処理を終了する。

【００３４】

クライアント端末７、８、９、１０は、低レベルの暗号化を施した無線通信によるリンクが破棄された後、リンク中に受信した認証用アカウントまたは証明書を利用して、ＥＡＰ等の認証プロセスを要する比較的高レベルな暗号化を施した無線通信を実施するための接続プロトコルを自動的に開始する。

【００３５】

尚、このとき、クライアント端末７、８、９、１０は、前回の比較的低レベルな暗号化を施した無線通信によるリンクを行った場合と同一のＥＳＳ　ＩＤを用いて、ＥＡＰ等の認証プロセスを要する比較的高レベルな暗号化を施した無線通信への移行を行う。これは、認証用アカウントまたは証明書の発行を行ったアクセスポイント１に、クライアント端末７、８、９、１０を確実に誘導して接続するためである。

【００３６】

図６はＥＡＰによる認証を行う際、クライアント端末７、８、９、１０、アクセスポイント１内の無線通信部２、アクセスポイント１内の認証サーバ３の遷移を示す図である。クライアント端末７、８、９、１０は、アクセスポイント１内の無線通信部２を介してアクセスポイント１内の認証サーバ３に２回のＥＡＰ－Ｒｅｓｐｏｎｓｅ（２００、２０１）を送信する。

【００３７】

これにより、アカウントとパスワードのセット、または証明書データの送信を行い、自身が認証サーバに登録されているクライアント端末であることの認証を行う。その結果、認証に合格すると、クライアント端末のネットワークアクセスが許可され、その後、クライアント端末７、８、９、１０とアクセスポイント１内の無線通信部２との間に設定されるＷＥＰキーを、一定時間毎に動的に変更することで、比較的高レベルな暗号化を施した無線通信を実現することができる。

【００３８】

尚、第１の実施形態では、アクセスポイント１の表示部５を利用し、比較的低レベルの暗号化を施した無線接続を実施する際のＩＤやＣｏｄｅ等のキーワード表示、ＰＡＮ参加者の編集時の一覧表示などを実施する旨の記述を行ったが、この表示は、有線ネットワークによるＰＡＮ構築用インターフェース１１９、１２０、１２１、１２２に接続されたクライアントデバイスに、ＷＥＢブラウザを利用して間接的に表示することも可能である。この場合、アクセスポイント１に表示部や入力用スイッチなどを具備する必要が無くなるので、コスト削減に有効である。

【００３９】

［第２の実施形態］

前記第１の実施形態では、新規にＰＡＮを構築する際の動作について示したが、第２の実施形態では、実際にＰＡＮを構築する際の動作として、会議を例に挙げ、会議開催時のＰＡＮに必要とされる機能の観点から説明する。

【００４０】

ここで、会議開催時にクライアント端末を相互に接続するＰＡＮを構築する場

合、前記第１の実施形態で示したように、比較的高レベルな暗号化を施した無線接続を利用することは、ユーザの利便性の点から非常に好ましい。

【００４１】

会議用ＰＡＮを構築する場合、各ユーザに発行するアカウントや証明書は、恒久的なものではなく、会議中だけ一時的に有効なものであることが必要である。このため、会議用にアクセスポイントを用いる場合、図４のステップＳ１で新しいＰＡＮの構築要求があった後、ステップＳ２の処理を行う前に、ＰＡＮ管理責任者による会議予定時間の入力のステップ処理を追加する。

【００４２】

この入力処理を追加することで、アカウントの有効時間を認証サーバに設定したり、発行する証明書の有効時間を証明書内のパラメータとして反映させることで、認証プロセスを要する比較的高レベルの暗号化を施した無線接続によるＰＡＮに有効時間を与えることができる。

【００４３】

また、前記第１の実施形態で示したように、ＰＡＮの管理責任者による確認作業が終了すると、ＰＡＮは、ＭＡＣアドレスフィルタリング等の処理によってロック状態となり、新たなユーザ参加を認めなくなる。

【００４４】

しかし、アクセスポイント１を会議等の環境下で用いる場合、一旦、ロック状態とした後、遅刻者の追加等の理由により、クライアント端末を追加するケースが考えられる。このような場合、ＰＡＮの管理責任者が、遅刻者を視認した際、アクセスポイント１を直接操作するか、あるいは管理責任者が使用しているクライアント端末９のＷＥＢブラウザを利用してアクセスポイント１の管理画面を起動し、間接的にアクセスポイント１を操作して、ロック状態を解除する。

【００４５】

図７は第２の実施形態における個人識別情報の一覧表示を示す図である。この画面上には、図５の画面と比べ、「ロック解除」ボタン３１が設けられている。この「ロック解除」ボタン３１をクリックすることにより、ＰＡＮのＭＡＣアドレスフィルタによる参加制限が解除される。

【００４６】

また、このとき、ＰＡＮ管理責任者は、遅刻者に対し、図中、Ｋｅｙｗｏｒｄとして表示されるＩＤやＣｏｄｅ情報を伝える。ここでは、Ｋｅｙｗｏｒｄは「ＧＣＳｍｅｅｔ」である。この後、追加でＰＡＮに参加しようとするユーザは、自身の所有するクライアント端末でアプリケーションを起動し、Ｋｅｙｗｏｒｄを入力する。ここで入力するキーワードは、前記第１の実施形態で示したように、比較的低レベルの暗号化を施した無線接続を実施する際、各ユーザが入力するＥＳＳ　ＩＤ、ＷＥＰキー、あるいはＰｉｎコード等の８０２．１１やＢｌｕｅｔｏｏｔｈによる無線通信を暗号化するためのパラメータそのものでもよい。本実施形態では、最終的にそれらのパラメータに自動変換されるキーワードが用いられている。

【００４７】

図８は第２の実施形態における８０２．１１方式による追加クライアントの無線接続を確立する処理手順を示すフローチャートである。ロック解除要求が行われたか否かを判別する（ステップＳ１１）。ロック解除要求が行われた場合、アクセスポイント１は、８０２．１１方式による低レベルの暗号化を施した無線通信に必要なパラメータであるＥＳＳ　ＩＤとＷＥＰキーを表示する（ステップＳ１２）。

【００４８】

クライアント端末にキーワードを入力すると、このクライアント端末は、既にその他のユーザによってＰＡＮが形成されているアクセスポイントに対し、低レベルの暗号化が施された無線接続を試みる。アクセスポイント１は、ＰＡＮに追加・参加しようとするクライアント端末を認識すると、画面表示を更新し、追加参加ユーザの個人情報を一覧に追記する（ステップＳ１３）。

【００４９】

尚、この追記は、図７の「更新」ボタン３２がクリックされたときに行われてもよい。ＰＡＮ管理責任者は、更新された一覧表示を確認し、仮に、不正ユーザが表示された場合、編集作業を行い、不正ユーザを削除する。すなわち、修正要求があるか否かを判別し（ステップＳ１４）、修正要求がある場合、修正作業を

行って（ステップＳ１５）、ステップＳ１３の処理に戻る。一方、修正要求がないとして、確認作業完了が入力された場合、ステップＳ１６の処理に移行する。

【００５０】

前記第１の実施形態と同様、アクセスポイント１は、確認作業完了の入力が行われた場合、確認されたユーザ以外のＰＡＮ参加を拒絶するため、確認されたユーザのＭＡＣアドレス等を用いたハードウェア識別コードによるフィルタリング設定を更新する（ステップＳ１６）。また、アクセスポイント１は、同時に新たに確認された追加クライアント端末に対し、認証用アカウントまたは証明書の発行作業を行う（ステップＳ１７）。

【００５１】

追加クライアント端末に認証用アカウントまたは証明書を送信し（ステップＳ１８）、送信完了を待つ（ステップＳ１９）。送信が完了すると、アクセスポイント１は、追加クライアント端末に対し、現状の低レベルな暗号化を施した無線通信によるリンクを破棄し（ステップＳ２０）、認証処理を要する高レベルな暗号化を施した無線通信の開始に備え、本処理を終了する。

【００５２】

尚、遅刻者のＰＡＮへの追加作業を実施する際、その他のＰＡＮ参加者は、継続的に認証プロセスを要する比較的高レベルな暗号化を施した無線接続を維持しており、そのＰＡＮ上で作業を継続できることは言うまでもない。

【００５３】

また、追加クライアント端末は、低レベルの暗号化を施した無線通信によるリンクが破棄された後、リンク中に受信した認証用アカウントまたは証明書を利用し、ＥＡＰ等の認証プロセスを要する比較的高レベルな暗号化を施した無線通信を行うための接続プロトコルを自動的に開始する。このとき、追加クライアント端末は、前回の比較的低レベルな暗号化を施した無線通信によるリンクを行った場合と同一のＥＳＳ　ＩＤを用いて、アクセスポイント１と選択的に接続することは言うまでもない。

【００５４】

これにより、前記第１の実施形態と同様、追加クライアント端末は、アクセス

ポイント１内の無線通信部２を介してアクセスポイント１内の認証サーバ３に２回のＥＡＰ－Ｒｅｓｐｏｎｓｅ（２００、２０１）を送信することによって、アカウントとパスワードのセットまたは証明書データの送信を行い、自身が認証サーバに登録されているクライアント端末であることの認証を行う。

【００５５】

この結果、認証に合格すると、追加クライアント端末のネットワークアクセスが許可され、その後、一定時間毎に、ＷＥＰキーを動的に変更することで、比較的高レベルな暗号化を施した無線通信を実現することができる。

【００５６】

このように、認証プロセスを要する比較的高レベルな暗号化を施した無線接続を維持しながら、同時に比較的低レベルな暗号化を施した無線接続を構築するためには、独立して暗号化レベルを制御可能な無線通信装置が必要であるが、本実施形態のように、複数の無線通信拡張カードを装着できるアクセスポイントである場合、複数の無線通信拡張カードを装着することで容易に実現することができる。

【００５７】

また、異なる暗号化レベルによる無線通信を１チップで実現できるコントローラを用いる場合、アクセスポイントに複数の無線通信拡張カードを実装することなく、１枚の無線通信拡張カードだけで第２の実施形態に示した処理を行うことも可能である。

【００５８】

尚、本発明は、前述した実施形態の機能を実現するソフトウェアのプログラムコードをシステムあるいは装置に供給することによって達成される場合にも適用できることはいうまでもない。この場合、プログラムコード自体が本発明の新規な機能を実現することになり、そのプログラム自体およびそのプログラムを記憶した記憶媒体は本発明を構成することになる。

【００５９】

プログラムコードを供給する記憶媒体としては、ＲＯＭに限らず、例えばフレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ、不揮発

性のメモリカードなどを用いることができる。

【００６０】

【発明の効果】

本発明によれば、アカウントや証明書を事前に取得していないユーザに対しても、認証プロセスを要する比較的高レベルな暗号化を施した無線接続システムを容易に構築できる。特に、会議等で一時的に安全なネットワークを構築したい場合に好適である。

【００６１】

このように、８０２．１ｘ認証・暗号化方式などの認証プロセスを要する、比較的安全性の高い暗号化方式による無線通信を用いたＰＡＮ構築を、認証プロセスに対応したアカウントや証明書を事前に所有していないクライアント端末においても実現可能である。

【００６２】

また、ＰＡＮ構築の際に利用する無線通信手段を簡単に選択できる。さらに、ＰＡＮ構築の際、無線通信手段を複数同時に利用可能とし、異なる無線通信手段で構成されたＰＡＮを簡単に構築することである。また、１枚のカードで対応できるユーザ数を越えたクライアント数によるＰＡＮの構築やクライアントの負荷分散を実現できる。したがって、ＰＡＮに参加可能な無線通信手段におけるクライアントの総数を増加させることができる。

【００６３】

さらに、無線通信手段によって構築したＰＡＮを、イントラネットやインターネットなどの基幹ネットワークに接続する場合、不正なアクセスを相互に禁止することができる。また、本アクセスポイントを製品化する場合のコストを低減できる。

【００６４】

さらに、アカウントや証明書を事前に所有していないクライアント端末によって、認証プロセスを要する比較的安全性の高い暗号化方式を用いた無線通信によるＰＡＮを構築する際、クライアントの操作を容易にすることができる。また、アカウントや証明書を事前に所有していないクライアント端末と、アクセスポイ

ントを接続する際のアクセスポイント側の設定操作を容易にすることができる。

【００６５】

また、構築された無線通信によるＰＡＮのクライアントに矛盾がないか否かの最終確認手段を提供できる。さらに、無線通信によるＰＡＮに参加可能なクライアント条件が、確認後に無断で変更できないようにすることができる。したがって、無線通信によるＰＡＮに対するクライアントの追加を無断で実行できないようにすることができる。また、認証プロセスを要する比較的高レベルな暗号化手段による無線通信へ移行する際、そのクライアントに対する認証を実施可能なアクセスポイントへ選択的に無線接続することができる。

【図面の簡単な説明】

【図１】

第１の実施形態におけるアクセスポイント装置およびクライアント端末によって構築されるネットワークシステムを示す図である。

【図２】

アクセスポイント１の構成を示すブロック図である。

【図３】

アクセスポイント装置のソフトウェアの構成を示す図である。

【図４】

８０２．１１方式による無線接続を確立する処理手順を示すフローチャートである。

【図５】

個人識別情報の一覧表示を示す図である。

【図６】

ＥＡＰによる認証を行う際、クライアント端末７、８、９、１０、アクセスポイント１内の無線通信部２、アクセスポイント１内の認証サーバ３の遷移を示す図である。

【図７】

第２の実施形態における個人識別情報の一覧表示を示す図である。

【図８】

第２の実施形態における８０２．１１方式による追加クライアントの無線接続を確立する処理手順を示すフローチャートである。

【符号の説明】

１　アクセスポイント装置

２　無線通信部

３　認証サーバ

４　証明書サーバ

７、８　ＰＤＡ

９、１０　ＰＣ

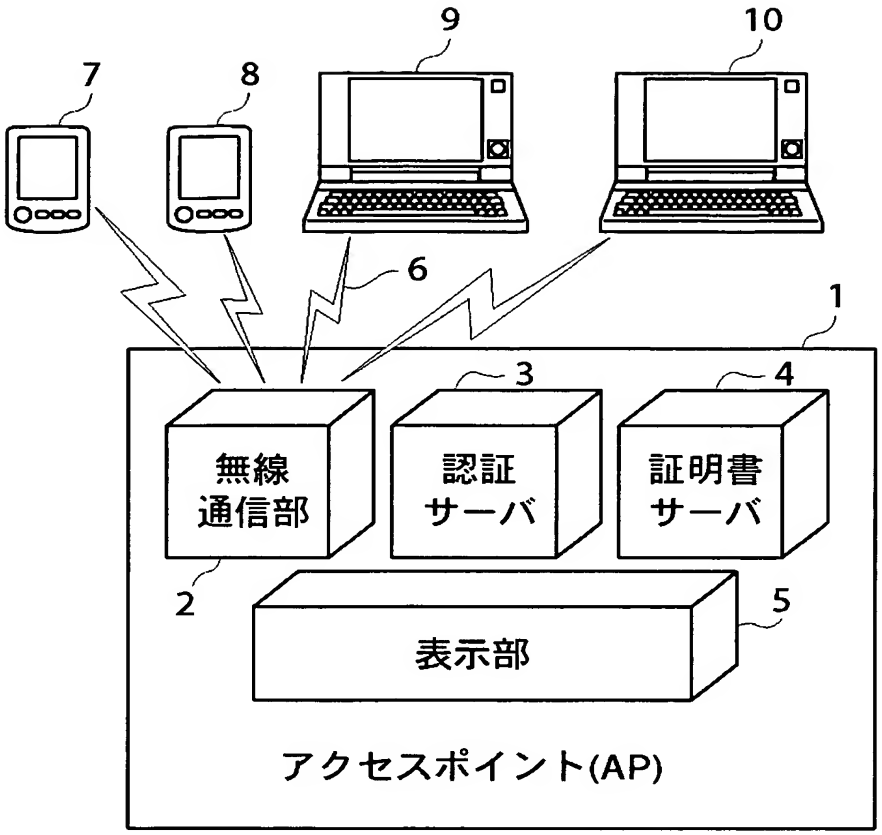
１０１　ＣＰＵ

１１０～１１３　拡張バスインターフェース

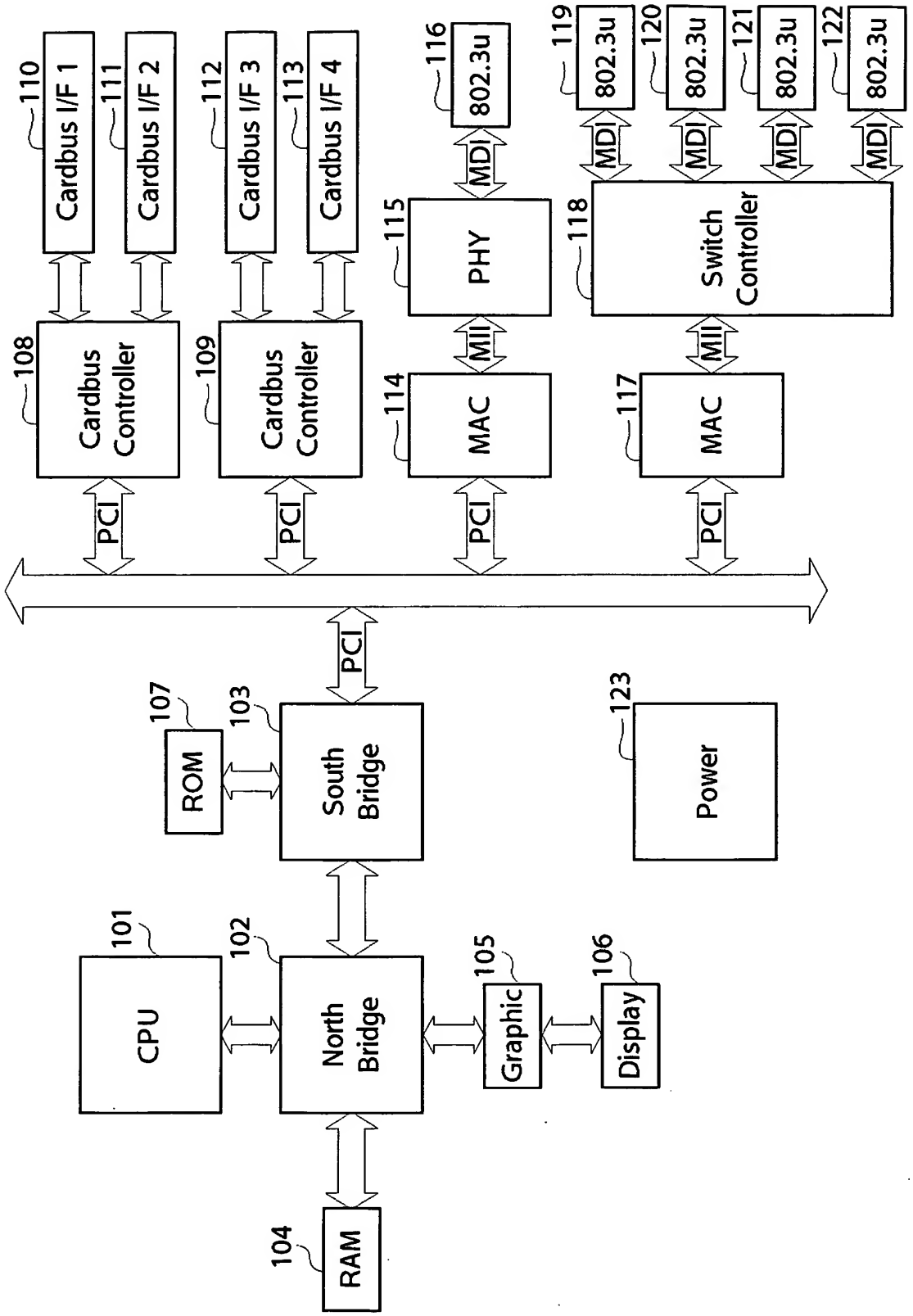
１１９～１２２　ＰＡＮ構築用インターフェース

【書類名】　図面

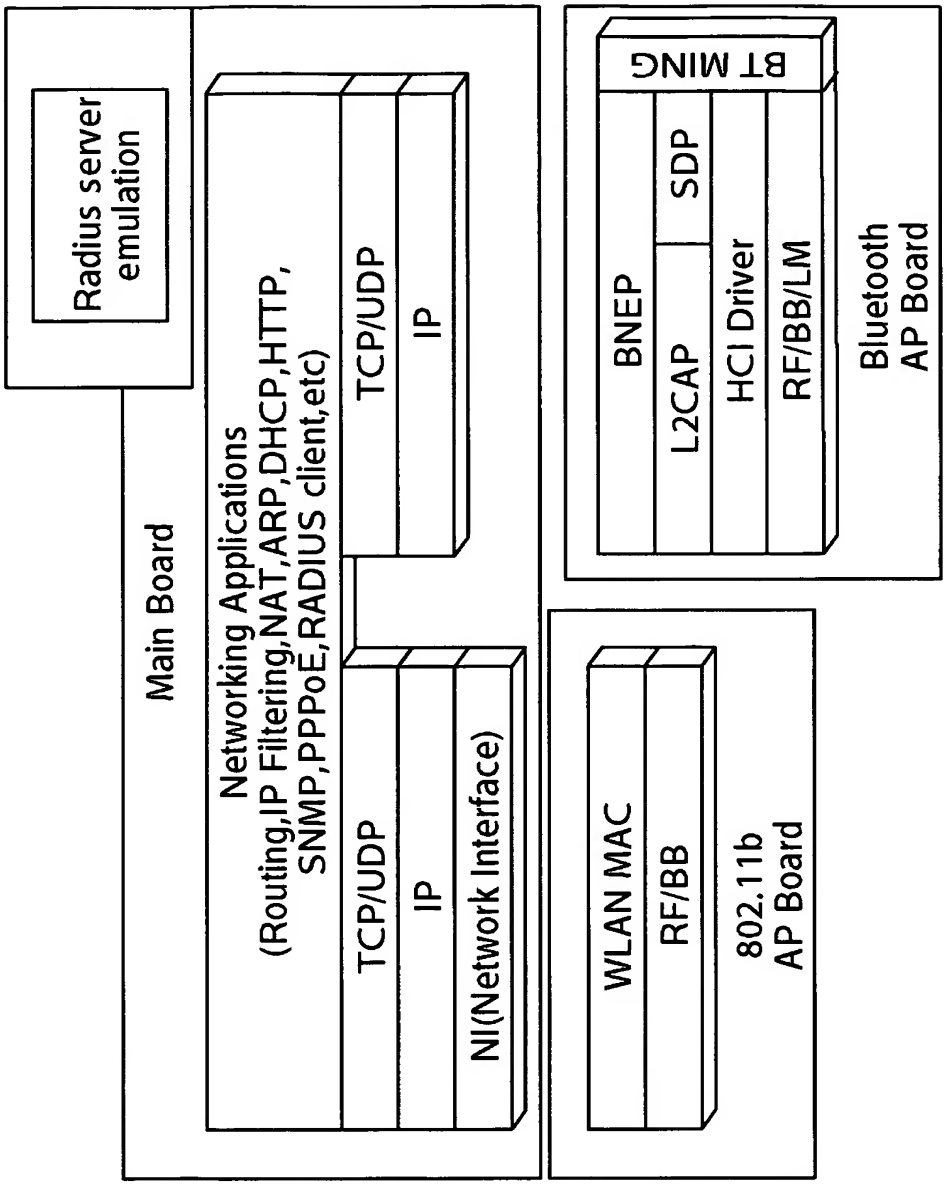
【図１】



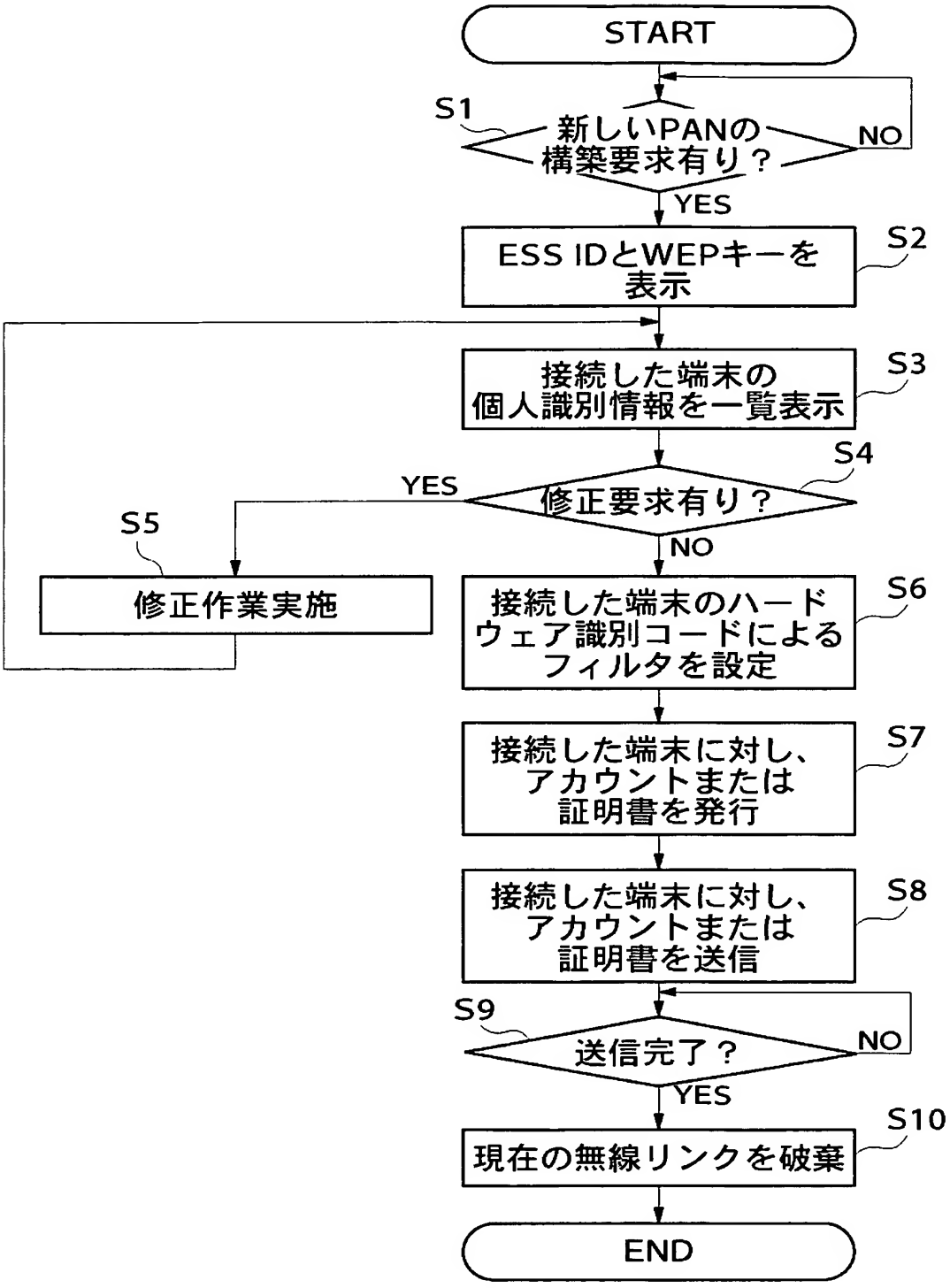
【図２】


110
Cardbus I/F 1
111
Cardbus I/F 2
112
Cardbus I/F 3
113
Cardbus I/F 4
116
802.3u
119
802.3u
120
802.3u
121
802.3u
122
802.3u
MDI
MDI
MDI
MDI
MDI
115
PHY
118
Switch Controller
108
Cardbus Controller
109
Cardbus Controller
MII
MII
114
MAC
117
MAC
PCI
PCI
PCI
PCI
PCI
107
ROM
103
South Bridge
123
Power
101
CPU
102
North Bridge
105
Graphic
106
Display
104
RAM

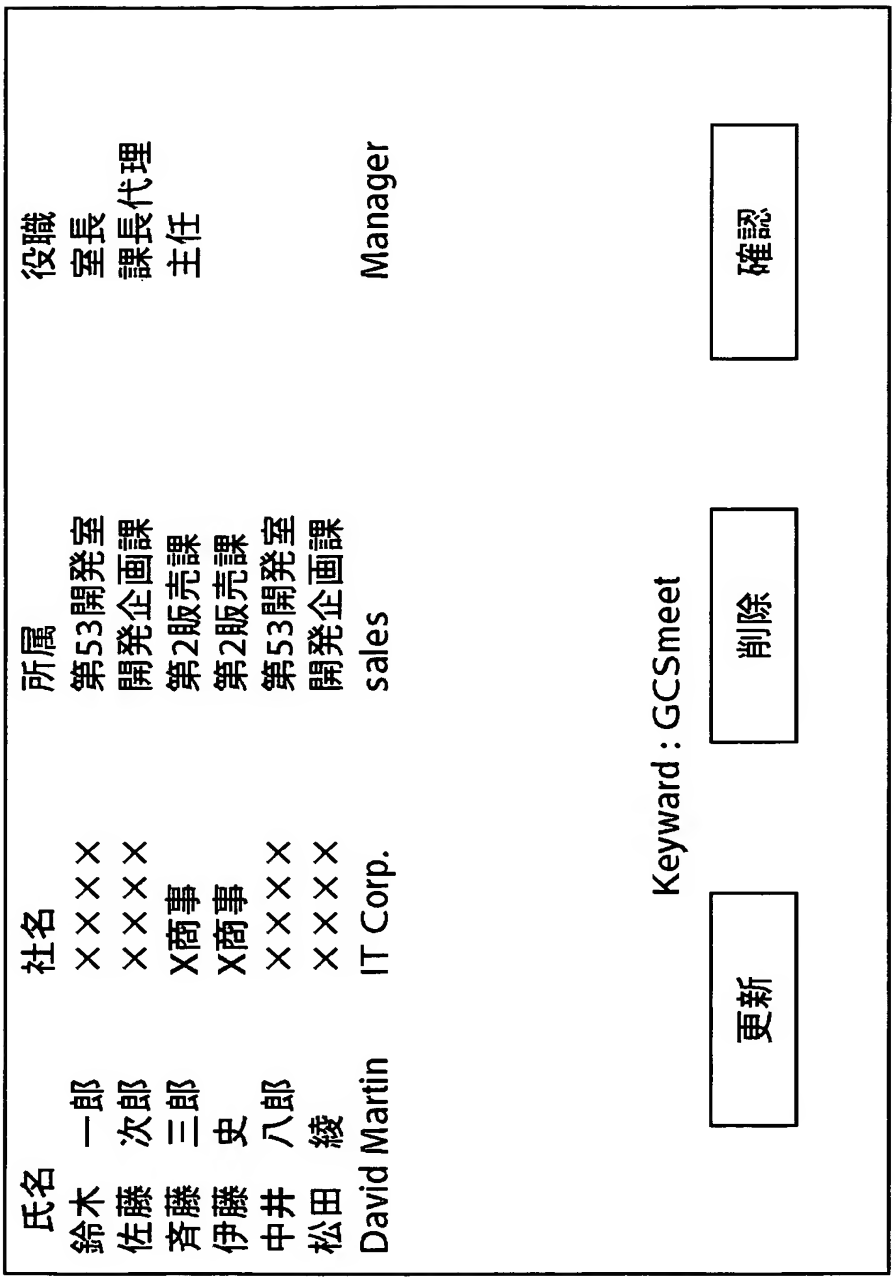
【図３】


Radius server emulation
Main Board
Networking Applications
(Routing,IP Filtering,NAT,ARP,DHCP,HTTP,
SNMP,PPPoE,RADIUS client,etc)
TCP/UDP
IP
TCP/UDP
IP
NI(Network Interface)
BT MING
BNEP
L2CAP
SDP
HCI Driver
RF/BB/LM
Bluetooth
AP Board
WLAN MAC
RF/BB
802.11b
AP Board

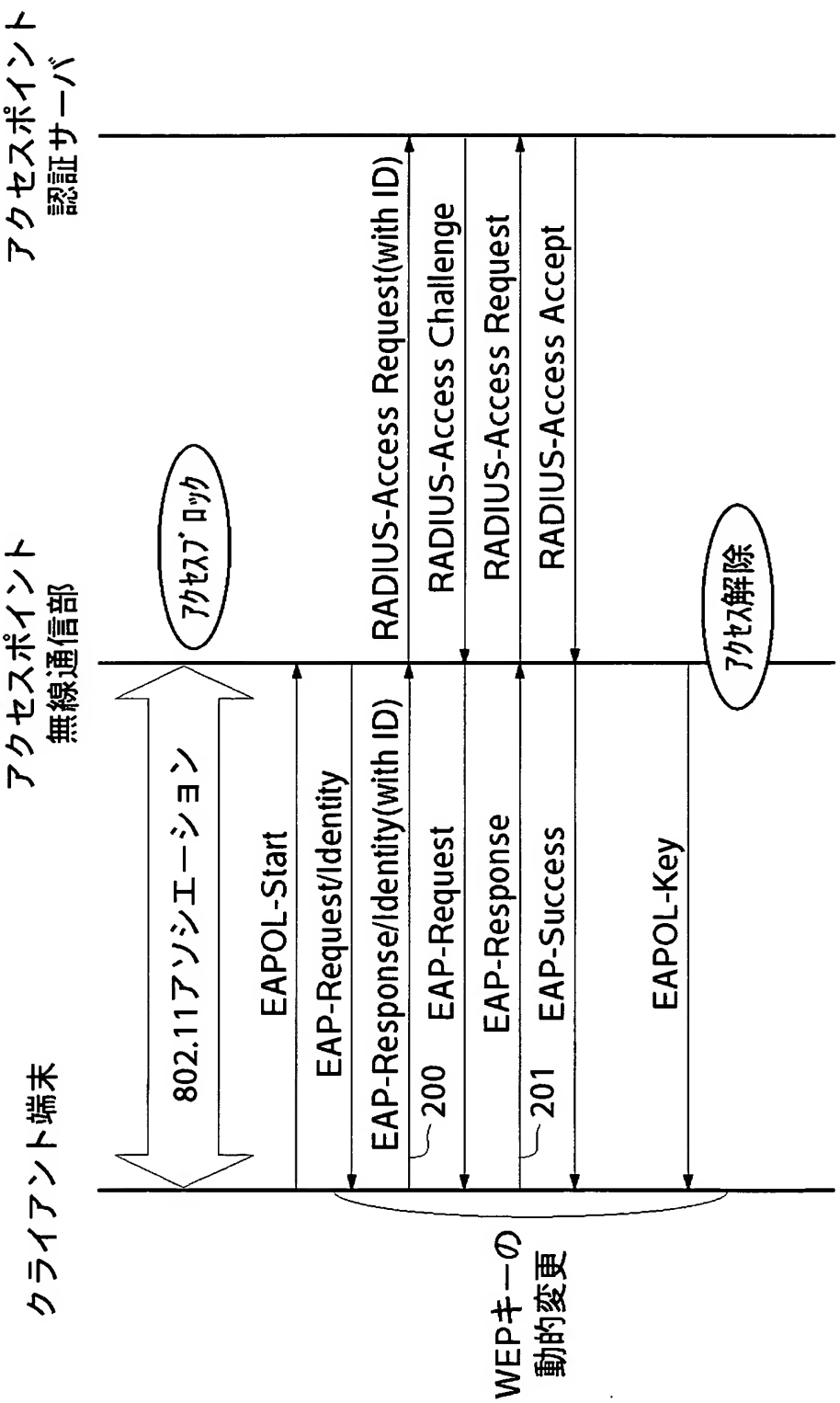
【図４】


START
S1
新しいPANの構築要求有り？
NO
YES
ESS IDとWEPキーを表示
S2
接続した端末の個人識別情報を一覧表示
S3
S4
修正要求有り？
YES
NO
S5
修正作業実施
接続した端末のハードウェア識別コードによるフィルタを設定
S6
接続した端末に対し、アカウントまたは証明書を発行
S7
接続した端末に対し、アカウントまたは証明書を送信
S8
S9
送信完了？
NO
YES
S10
現在の無線リンクを破棄
END

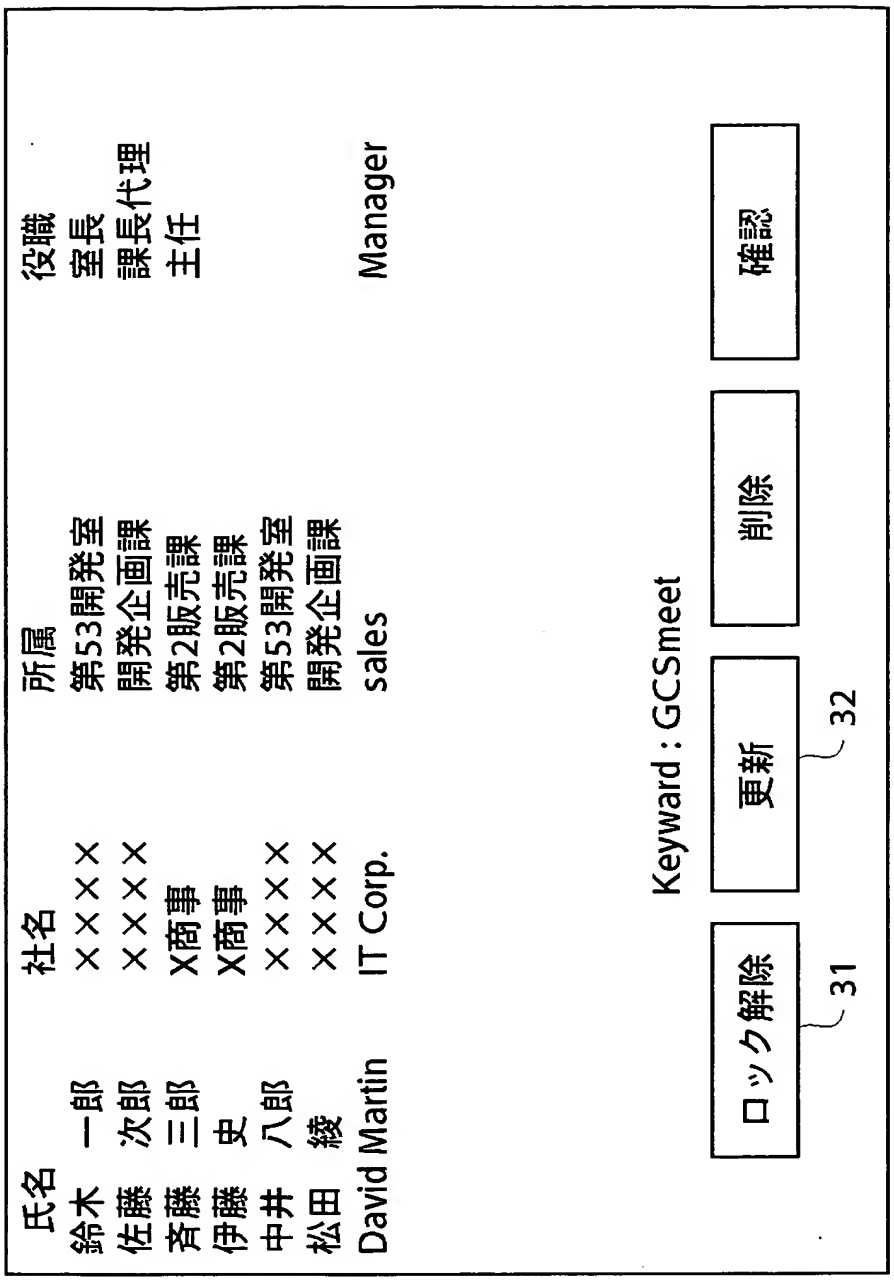
【図５】


氏名
社名
所属
役職
鈴木　一郎　××××　第53開発室　室長
佐藤　次郎　××××　開発企画課　課長代理
斉藤　三郎　X商事　第2販売課　主任
伊藤　史　X商事　第2販売課
中井　八郎　××××　第53開発室
松田　綾　××××　開発企画課
David Martin　IT Corp.　sales　Manager
Keyward : GCSmeet
更新
削除
確認

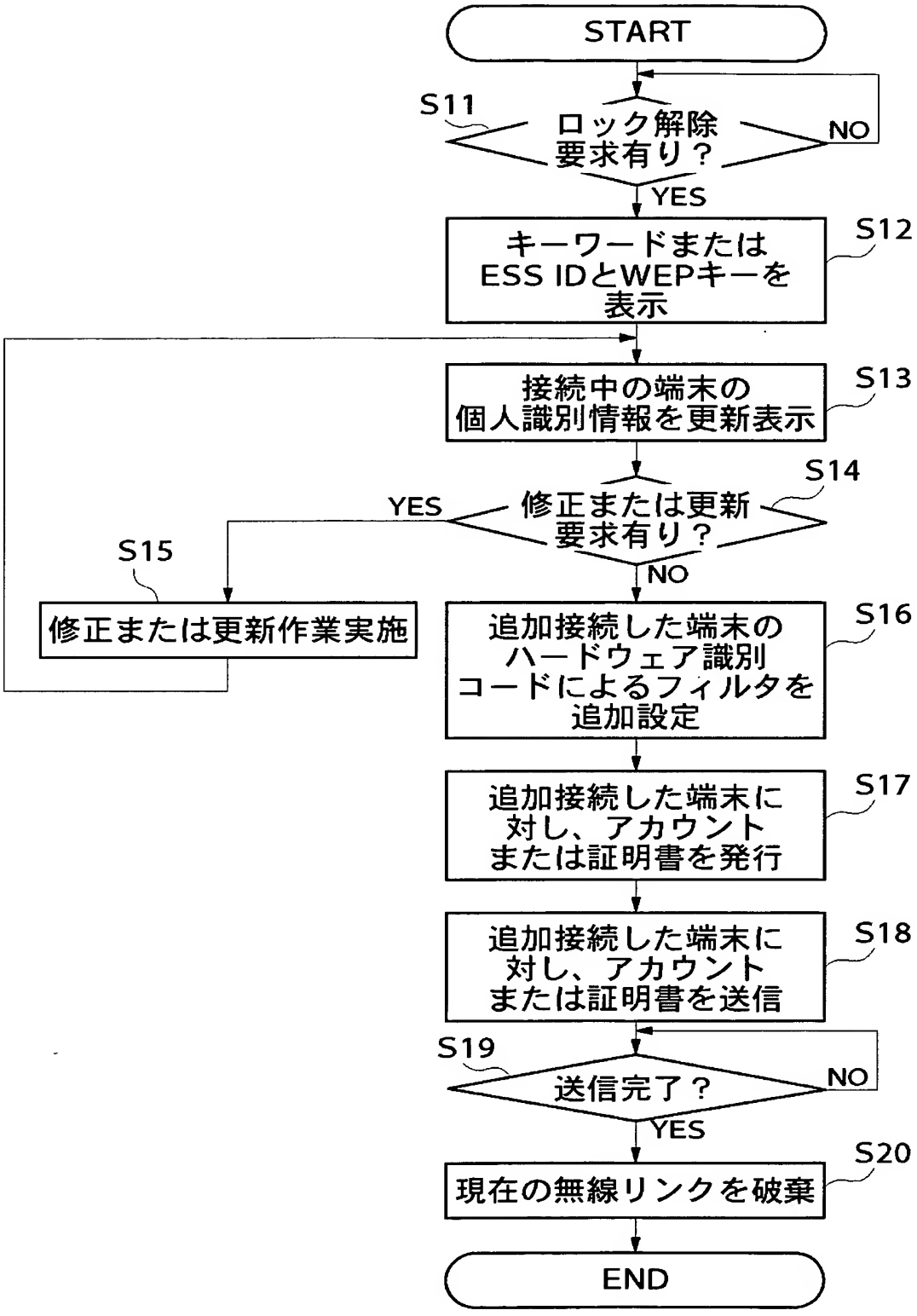
【図６】


クライアント端末
アクセスポイント
無線通信部
アクセスポイント
認証サーバ
802.11アソシエーション
アクセスブロック
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity(with ID)
RADIUS-Access Request(with ID)
200
EAP-Request
RADIUS-Access Challenge
EAP-Response
RADIUS-Access Request
201
EAP-Success
RADIUS-Access Accept
EAPOL-Key
アクセス解除
WEPキーの
動的変更

【図７】


氏名　社名　所属　役職
鈴木　一郎　××××　第53開発室　室長
佐藤　次郎　××××　開発企画課　課長代理
斉藤　三郎　X商事　第2販売課　主任
伊藤　史　X商事　第2販売課
中井　八郎　××××　第53開発室
松田　綾　××××　開発企画課
David Martin　IT Corp.　sales　Manager
Keyward : GCSmeet
ロック解除
31
更新
32
削除
確認

【図８】


START
S11
ロック解除
要求有り？
NO
YES
キーワードまたは
ESS IDとWEPキーを
表示
S12
接続中の端末の
個人識別情報を更新表示
S13
S14
修正または更新
要求有り？
YES
NO
S15
修正または更新作業実施
追加接続した端末の
ハードウェア識別
コードによるフィルタを
追加設定
S16
追加接続した端末に
対し、アカウント
または証明書を発行
S17
追加接続した端末に
対し、アカウント
または証明書を送信
S18
S19
送信完了？
NO
YES
現在の無線リンクを破棄
S20
END

【書類名】　　要約書

【要約】

【課題】　比較的安全性の高い暗号化方式による無線通信を用いたＰＡＮ構築を、認証プロセスに対応したアカウントや証明書を事前に所有していないクライアント端末においても実現可能であるアクセスポイント装置を提供する。

【解決手段】　比較的低レベルな暗号化方式による無線通信のリンクをクライアント端末との間で確立した後、認証プロセスを必要とする高レベルな暗号化方式による無線通信を行うために必要な認証用データをクライアント端末に送信し、一旦リンクを破棄する。再度、認証用データを用いて安全な無線通信によるＰＡＮを再構築する。

【選択図】　　図１

特願２００２－２３３１１９

出　願　人　履　歴　情　報

識別番号　　［０００００１００７］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都大田区下丸子３丁目３０番２号
氏　名　　キヤノン株式会社